AO 106 (Rev. 4/10) Application for a Search Warrant

# UNITED STATES DISTRICT COURT
for the
EASTERN DISTRICT OF WISCONSIN

In the Matter of the Search of:

657 Greenway Terrace, Hartland, Wisconsin: a two story home with tan siding and light brown asphalt roof shingles, with the number 657 in black lettering affixed to the front of the residence, adjacent to the attached two-car garage.

APPLICATION & AFFIDAVIT FOR SEARCH WARRANT

Case Number: 12-m-518

I, Jason Pleming, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

> **657 Greenway Terrace, Hartland, Wisconsin**: a two story home with tan siding and light brown asphalt roof shingles, with the number 657 in black lettering affixed to the front of the residence, adjacent to the attached two-car garage

located in the Eastern District of Wisconsin there is now concealed certain property, namely: those items listed in **Attachment A**.

The basis for the search warrant under Fed. R. Crim. P. 41(c) is which is (check one or more):

✓ evidence of a crime;
□ contraband, fruits of a crime, or other items illegally possessed;
□ property designed for use, intended for use, or used in committing a crime;
□ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of: Title 18, United States Code, Section 2252A.

The application is based on these facts:

✓ Continued on the attached affidavit, which is incorporated by reference.

□ Delayed notice of ____ days (give exact ending date if more than 30 days:_________) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Name: JASON PLEMING
Title: Special Agent United States Department of Justice, Federal Bureau of Investigation

Sworn to before me, and signed in my presence.

Date August 21st, 2012 at 9:20AM
City and state: Milwaukee, Wisconsin

William E Callahan
THE HONORABLE WILLIAM E. CALLAHAN, JR.
United States Magistrate Judge

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Jason Pleming, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

1. I have been employed with the FBI as a sworn law enforcement officer since September 2006. I am currently assigned to the Milwaukee Division Cyber Crimes Task Force (CCTF). I am charged with conducting investigations of violations of federal law including the receipt, possession, distribution, and production of child pornography. I have gained experience in the conduct of such investigations through prior investigations, formal training, and in consultation with other members of the CCTF regarding these matters.

2. As a FBI Special Agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. This affidavit is being submitted in support of an Application for a Search Warrant for the residence located at 657 Greenway Terrace, Hartland, Wisconsin (hereinafter, "PREMISES"), in the State and Eastern District of Wisconsin, for evidence of violations of Title 18, United States Code (USC) § 2252A, entitled "Certain activities relating to material constituting or containing child pornography."

4. Based upon the information summarized in this affidavit, I have reason to believe that evidence of such violations may be present at the residence located at 657 Greenway Terrace, Hartland, Wisconsin .

5. The information supplied in this affidavit is based upon my investigation and information provided and investigation conducted by other law enforcement personnel in this matter to date. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not set forth every fact related to or otherwise the product of this investigation.

DEFINITION OF TECHNICAL TERMS

6. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, floppy disks, flash memory, CD-ROMs, and several other types of magnetic or optical media not listed here.

d. Globally Unique Identifier (GUID) / User Hash: A GUID/User Hash is a special type of identifier used in software applications to provide a unique reference number.

e. Peer-to-Peer Network (P2P): A P2P network allows users to trade digital files through a worldwide network formed by linking computers together via special software. Typically, users perform a keyword search to locate files, and the files can then be downloaded from any users in possession of those files. Users cannot send or receive files without consent.

f. Hash Algorithm: Files being shared by P2P clients are processed by the client software. As part of this processing, a hashed algorithm value (i.e. MD5, SHA-1, and eD2K MD4) is computed for each file being shared, which uniquely identifies it on the network. A file processed by this hash algorithm operation results in the creation of an associated hash value often referred to as a digital signature. Some hash algorithms provide a certainty exceeding 99.99 percent that two or more files with the same hash value are identical copies of the same file regardless of their file names. The slightest alteration of any file will result in a completely different hash value. By using a hash algorithm to uniquely identify files on a P2P network, it improves the network efficiency. Because of this, typically, users may receive a selected file from numerous sources by accepting segments of the same file from multiple clients and then reassembling the complete file on the local computer. This is referred to as multiple source downloads. The client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. P2P file sharing networks use hash values to ensure exact copies of the same file are used during this process.

g. Computer Ports: In computer networking, the term port can refer to either a physical or virtual connection point. Physical network ports allow connecting cables between computers, routers, modems and other peripheral devices. Virtual ports are part of TCP/IP networking. These ports allow software applications to share hardware resources without interfering with each other. Computers and routers automatically manage network traffic traveling via their virtual ports. Network firewalls additionally provide some control over the follow of traffic on each virtual port for security purposes. A port number is part of the addressing information used to identify the senders and receivers of messages. Port numbers are most commonly used with TCP/IP connections. Home network routers and computer software work with ports and sometimes allow you to configure port number settings. These port numbers allow different applications on the same computer to share network resources simultaneously. Port numbers are also associated with network addresses. For example, in TCP/IP networking, both TCP and UDP utilize their own set of ports that work together with IP addresses. Port numbers work like telephone extensions. Just as a business telephone switchboard can use a main phone number and assign each employee an extension number (like x100, x101, etc.), so a computer has a main address and a set of port numbers to handle incoming and outgoing connections. In both TCP and UDP, port numbers start at 0 and go up to 65535. Numbers in the lower ranges are dedicated to common Internet protocols (like 21 for FTP and 80 for HTTP).

PROBABLE CAUSE

7. Between May 29, 2012 and July 29, 2012, SA Pleming, while connected to the Internet in an online undercover capacity, conducted numerous online investigations to identify those individuals possessing and sharing child pornography using the eDonkey2000 (eD2K) and Kademlia (KAD) peer to peer networks. SA Pleming utilized a Peer to Peer (P2P) file sharing program, which scans both networks simultaneously and has been enhanced to ensure that downloads occur only from a single selected source.

8. During those investigations, SA Pleming searched for suspected child pornography files and identified IP address 75.35.49.88 on the KAD network, with a User Hash of 6650E7B4600E0095C9E7B6E494B26F7A, which had suspected child pornography files available for distribution. Specifically, IP address 75.35.49.88 responded to SA Pleming's queries for the following suspected child pornography eD2K hash values (also utilized by the KAD network) on their respective dates and times, as outlined in the table below.

Date	Time	User Hash	File (ed2k MD4 Hash)	IP
5/29/2012	22:01:38	6650E7B4600E0095C9E7B6E494B26F7A	68CBF7A70563BA508BCCE50A938EC93E	75.35.49.88
6/20/2012	5:47:41	6650E7B4600E0095C9E7B6E494B26F7A	5CAABB7DE4338853329FF0C0A0AD449D	75.35.49.88
6/20/2012	6:57:49	6650E7B4600E0095C9E7B6E494B26F7A	B075C98DE545D3F83B24D67E70B5E454	75.35.49.88
6/27/2012	7:49:06	6650E7B4600E0095C9E7B6E494B26F7A	D9C656C4D404AD01288987E3D93F8827	75.35.49.88
7/09/2012	8:50:08	6650E7B4600E0095C9E7B6E494B26F7A	FBD20FD5962BB93A83A99C1AB4ECACDD	75.35.49.88
7/10/2012	17:24:27	6650E7B4600E0095C9E7B6E494B26F7A	EB2D94E20C82103BD958220F75F657F5	75.35.49.88
7/13/2012	14:09:58	6650E7B4600E0095C9E7B6E494B26F7A	FBD20FD5962BB93A83A99C1AB4ECACDD	75.35.49.88
7/13/2012	18:13:34	6650E7B4600E0095C9E7B6E494B26F7A	629DAB4232B64839E19D1B6BD17D7E68	75.35.49.88
7/14/2012	5:37:26	6650E7B4600E0095C9E7B6E494B26F7A	629DAB4232B64839E19D1B6BD17D7E68	75.35.49.88
7/22/2012	20:02:33	6650E7B4600E0095C9E7B6E494B26F7A	0374497898F9014FF0DE3CB7113FEA65	75.35.49.88
7/23/2012	12:26:42	6650E7B4600E0095C9E7B6E494B26F7A	6C13C50A47E6A52AA007EC360802F719	75.35.49.88
7/23/2012	14:52:29	6650E7B4600E0095C9E7B6E494B26F7A	E9B436D6C84AE59FBD0614C7CAE22A44	75.35.49.88
7/23/2012	17:02:20	6650E7B4600E0095C9E7B6E494B26F7A	41C026B4BD13EBFBB7C23DBD0DC5CA2A	75.35.49.88
7/23/2012	17:58:09	6650E7B4600E0095C9E7B6E494B26F7A	ADA3C71998AF7858FF1AC6A531E62D2F	75.35.49.88
7/24/2012	4:38:00	6650E7B4600E0095C9E7B6E494B26F7A	940A47113CF81BDEE1DD00F6E4C5ED98	75.35.49.88
7/27/2012	8:10:05	6650E7B4600E0095C9E7B6E494B26F7A	9D12D2C3E4BCBE28EEBDB5723D52034A	75.35.49.88
7/28/2012	3:20:03	6650E7B4600E0095C9E7B6E494B26F7A	629DAB4232B64839E19D1B6BD17D7E68	75.35.49.88
7/29/2012	23:53:20	6650E7B4600E0095C9E7B6E494B26F7A	629DAB4232B64839E19D1B6BD17D7E68	75.35.49.88
7/29/2012	23:53:20	6650E7B4600E0095C9E7B6E494B26F7A	629DAB4232B64839E19D1B6BD17D7E68	75.35.49.88

9. For each of the dates listed above in the referenced table, the Maxmind.com database reported that IP address 75.35.49.88 was registered to AT&T Internet Services. Further, the website reported that the aforementioned IP address was assigned to an address in Hartland, Wisconsin.

10. On July 31, 2012, the aforementioned suspected child pornography hashes were submitted to the National Center for Missing & Exploited Children (NCMEC) for preliminary identification. Since the files listed above were referenced by the eD2K MD4 hash values, SA Pleming obtained their MD5 hash value equivalent for submittal to the NCMEC. The table below gives the equivalent MD5 hash for each of the ed2k MD4 hashes.

ed2k MD4 Hash	MD5 Hash
68CBF7A70563BA508BCCE50A938EC93E	**82AFDC02A6A3D6B73FA1D31D664023A4**
5CAABB7DE4338853329FF0C0A0AD449D	C48FA7528E794BFC7602D385B52B337C
B075C98DE545D3F83B24D67E70B5E454	1E40ABB44F842472E5F266B29095974C
D9C656C4D404AD01288987E3D93F8827	33CEEFF17EEF23ED0BFBE800F87E2DDC
FBD20FD5962BB93A83A99C1AB4ECACDD	02E7D90CE689BC8BF240DEC47A91B8A0
EB2D94E20C82103BD958220F75F657F5	FDE9097291A00CDB51A3B9065063B5B6

FBD20FD5962BB93A83A99C1AB4ECACDD	02E7D90CE689BC8BF240DEC47A91B8A0
629DAB4232B64839E19D1B6BD17D7E68	3AE94E56F23E88DFD89359759E78CC0E
629DAB4232B64839E19D1B6BD17D7E68	3AE94E56F23E88DFD89359759E78CC0E
0374497898F9014FF0DE3CB7113FEA65	66646AF8DD702D9B81FEF33DF56D2E06
6C13C50A47E6A52AA007EC360802F719	407F22E9BF13699A32DE66DCF2E71EC9
E9B436D6C84AE59FBD0614C7CAE22A44	1B2456007474C04483F6A845664BD5AD
41C026B4BD13EBFBB7C23DBD0DC5CA2A	CB2F1B80B6C3C5254C1F6571244AC80D
ADA3C71998AF7858FF1AC6A531E62D2F	6750EF6EC56BE617C37EF522E07FB0CD
940A47113CF81BDEE1DD00F6E4C5ED98	86AD6629F91E7DFA62022A78343C9AE9
9D12D2C3E4BCBE28EEBDB5723D52034A	2A9BD4BBF4E37206A581689E797CBD30
629DAB4232B64839E19D1B6BD17D7E68	3AE94E56F23E88DFD89359759E78CC0E
629DAB4232B64839E19D1B6BD17D7E68	3AE94E56F23E88DFD89359759E78CC0E
629DAB4232B64839E19D1B6BD17D7E68	3AE94E56F23E88DFD89359759E78CC0E

11. On July 31, 2012, NCMEC advised that MD5 hash value **82AFDC02A6A3D6B73FA1D31D664023A4** matched a known child victim. The remaining hashes were identified as "Recognized," which meant they had been previously submitted to NCMEC as suspected child pornography by law enforcement.

12. While conducting this investigation, SA Pleming attempted without success to conduct single source downloads of the suspected child pornography files from IP address 75.35.49.88. SA Pleming noted that IP address 75.35.49.88 had been given a “low ID” designation on the KAD network. A “high ID” means the ports chosen within the P2P software program are open and freely accessible, whereas a “low ID” means these ports are blocked or cannot be reached. In most instances a client is assigned a “low ID” because they are behind a firewall or router without port forwarding enabled. It should be noted that being assigned a “low ID” will not prevent the P2P software user from downloading or trading files; however, to date SA Pleming has not been able to conduct single source downloads from users who have been assigned a “low ID.” Even though SA Pleming has not had success conducting a single source downloads with “low ID” clients, SA Pleming has had success with “low ID” clients responding to SA Pleming’s request for

suspected child pornography files, as shown in the table above.

13. As SA Pleming was unable to download the aforementioned digital files, SA Pleming then reviewed two digital files with the same eD2K MD4 hash values from his evidence library. The following is the description of the digital files and their corresponding eD2K MD4 hash values:

eD2K MD4 Hash: EB2D94E20C82103BD958220F75F657F5

> This video is approximately 10 seconds in length, and depicts a naked boy, approximately 6 years old, lying on his back while another naked boy, approximately 12 years old, performs oral sex on him.

eD2K MD4 Hash: 940A47113CF81BDEE1DD00F6E4C5ED98

> This video is approximately 8 minutes and 14 seconds in length, and begins with two minor males, both approximately 10 years old, wearing only their underwear, wrestling on a bed. Shortly thereafter, they remove their underwear and continue to wrestle and look at pornographic magazines on the bed. During the video, their penises are routinely the focal point of the camera, and towards the end of the video, one of the minor males begins to masturbate.

14. On July 25, 2012, AT&T Internet Services responded to subpoenas requesting subscriber information regarding IP addresses 75.35.49.88 on the date and times that child pornography was observed, as described above. AT&T provided the following subscriber information for said IP address: Mark A. Riesinger, 657 Greenway Terrace, Hartland, Wisconsin; phone number (262) 6XX-1XXX; length of service, October 15, 2008.

15. On August 01, 2012, SA Pleming went to the address of 657 Greenway Terrace, Hartland, Wisconsin to conduct surveillance and determine if there was a wireless connection which could be associated with this residence. A check of the available wireless connections when parked in front of the residence revealed that there were several secured wireless connection points that did not have an SSID (Service Set Identifier – a naming convention for wireless networks which requires that all wireless devices on a wireless network employ the same SSID in order to

communicate with each other) that could be associated with the residence. There were no unsecured wireless connection points found at this location, indicating that the suspect's wireless connection is secured, if the suspect is utilizing wireless internet. While conducting the surveillance, SA Pleming observed the following vehicles parked at the residence, which listed to the associated persons at that address by the Wisconsin Department of Transportation:

1. 2012 Silver Honda Accord, Wisconsin license plate 315-TNG; registered to Mark A. Riesinger, date of birth XX/XX/1955;
2. 2009 Light Brown Honda Accord, Wisconsin license plate 816-NTL; registered to Karla R. Riesinger, XX/XX/1957; and
3. 2008 Black Ford Mustang GT, Wisconsin license plate 240-NVY; registered to Erik J. Riesinger, XX/XX/1982.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

16. This application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

17. Probable cause. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

18. Forensic evidence. This application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

19. Necessity of seizing or copying entire computers or storage media. In most cases, a thorough search of the premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

20. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

21. Because it is possible that several people share the PREMISES as a residence, it is

possible that the PREMISES will contain computers that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

Statement of Probable Cause in Support of Application

22. Based on the facts as I have stated them in this affidavit, there is probable cause to believe that evidence of violations of Section 2252A of Title 18 of the United States Code is located at the residence 657 Greenway Terrace, Hartland, Wisconsin. "Attachment A" to this affidavit is a list of items that would be the subjects of search and seizure at this location.

23. The residence at 657 Greenway Terrace, Hartland, Wisconsin is more particularly described as follows: a two story home with tan siding and light brown asphalt roof shingles, with the number 657 in black lettering affixed to the front of the residence, adjacent to the attached two-car garage.

ATTACHMENT A

1. All records relating to violations of Title 18, United States Code, Sections 2252A, including:

   a. Records containing child pornography or pertaining to the distribution, receipt or possession of child pornography;

   b. Records evidencing occupancy or ownership of the premises described above, including but not limited to utility and telephone bills, mail envelopes, or addressed correspondence;

   c. Cellular telephones, telephone and address books, and other notes and papers insofar as they memorialize, include, or confirm computer screen names, contact information, or images related to the sexual exploitation of children, in violation of Title 18, United States Code, Section 2252A;

   d. Any and all records in any form or other items or materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence, including but not limited to sales receipts, invoices, bills for Internet access, and handwritten notes.

2. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

   a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment.

j. Records and things evidencing the use of the Internet Protocol addresses 75.35.49.88 including:

k. routers, modems, and network equipment used to connect computers to the Internet;

l. records of Internet Protocol addresses used;

m. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet or P2P search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

ATTACHMENT A

ADDENDUM TO SEARCH WARRANT

In searching for data capable of being read stored or interpreted by a computer, law enforcement personnel executing this search warrant will employ the following procedure:

a. Upon securing the premises, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") will make an initial review of any computer equipment and storage devices (collectively the "computer devices") to determine whether the computer devices can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data contained on the computer devices.

b. If the computer devices can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, they will be searched on-site, and a computer device will be seized only if the search reveals it to contain any data that falls within the list of items to be seized set forth herein.

c. If the computer devices cannot be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, then the computer devices will be seized and transported to an appropriate law enforcement laboratory for review. The computer devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein.

d. In searching the computer devices, the computer personnel may examine all of the data contained in the computer devices to view items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden" or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.

e. If the computer personnel seize the computer devices , the computer personnel will search the computer devices or data images within a reasonable amount of time not to exceed **30 days** from the date of execution of the warrant. If, after conducting such a search, the case agents determine that a computer device contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the computer device; otherwise, the government will return the computer device. If the government establishes a need for additional time to determine whether the data on the computer devices falls within any of the items to be seized pursuant to this warrant, it may seek an extension of the time period from the court within the original thirty day period from the date of execution of the warrant.